Review of Bachelor's Thesis

Student: Beránek Tomáš
Title: Practical Application of Facebook Infer on Systems Code (id 24187)
Reviewer: Malík Viktor, Ing., DITS FIT BUT

1. **Assignment complexity** — **more demanding assignment**
   The assignment complexity is slightly above average, mainly because it requires (1) to study and to understand advanced program analysis techniques and (2) to deeply investigate the code of a number of real-world software projects, many of which contain a lot of legacy code which is notoriously hard to understand.
2. **Completeness of assignment requirements** — **assignment fulfilled with enhancements**
   The thesis covers all points of the assignment and it contains an additional extension (incremental analysis wrapper) which was not mentioned in the assignment and which significantly improves the applicability of Facebook Infer on real-world projects.
3. **Length of technical report** — **in usual extent**
   The thesis has about 50 pages which is close to the upper bound of the required scope. The contained information is mostly useful, however, some parts are not necessary and they could have been shortened or omitted. This applies mainly to Section 2.2 which did not need to describe all Infer's plugins (especially not the unused or deprecated ones) and Section 4.1 whose subsections (1) often simply rewrite the information already shown in tables and (2) contain a number of very similar paragraphs (e.g., information about the given project's version, age, size, or references to appendices) which could have been summarized in a table.
4. **Presentation level of technical report** — **75 p. (C)**
   The thesis consist of several parts and each of them is described in a separate chapter. While some chapters are quite easy to follow, others are a bit difficult to read and they sometimes miss important information.

   The most notable problems are:
   - Section 3.4 completely misses motivation or data that would support the selection of the implemented filters.
   - Algorithm 5.1 is not well structured - procedural code is mixed with definition of a function, variables are non-initialized, compound variables have unclear structure, etc.
   - Algorithm 5.2 could be written in a much simpler way. Also, it contains an iteration over a data structure which is modified inside the same loop, which is not a good practice and has unclear behavior.
   - Chapter 6 misses some results of the experiments (at least numbers of reported/filtered issues).
5. **Formal aspects of technical report** — **80 p. (B)**
   The thesis is written in English and it is easy to understand, although there is a number of linguistic mistakes (sentences are lacking verbs, commas are misused or unused, etc.). The typography of the thesis is good.
6. **Literature usage** — **90 p. (A)**
   The thesis contains 41 references, mostly academic papers and web resources of Facebook Infer. The references are used in a correct and sufficient way.
7. **Implementation results** — **90 p. (A)**
   The thesis provides two implementation results (an Infer plugin for Csmock and an incremental analysis wrapper for Infer) and two experimental evaluations of Infer (on SRPM packages and on other open-source projects). Particularly the evaluation on SRPM packages is very thorough and extensive, the student manually investigated hundreds of reported issues to verify their correctness. Thanks to this, the implemented filters are able to remove a substantial amount of false positives. The only shortcoming is the lack of an experimental evaluation for the incremental analysis wrapper.
8. **Utilizability of results**
   The solutions implemented in the thesis identify and mitigate the most serious problems of applicability of Facebook Infer on real world projects. The thesis is a great step toward practical usability of Infer, especially in the context of Unix system utilities. The proposed extensions are directly usable in practice, which is supported by the fact that the student was able to use them to discover actual bugs in widely spread software (such as zip or less).
9. **Questions for defence**
   1. Based on which criteria you selected the filters to implement?
   2. Did you consider implementing the proposed methods (a better incremental analysis or TP filtering) directly

in Infer? How difficult would that be?

10. Total assessment

87 p. very good (B)

The thesis provides several good-quality solutions for non-trivial practical problems. In addition, benefits of the work are demonstrated in a very detailed experimental study which helped to discover new bugs in widespread software tools. The only drawback is the text part which feels a little unfinished and which spoils the overall impression of the work. Overall, I suggest to rate the thesis by the **grade B**, but I think that the committee may consider an even better evaluation in case of an excellent presentation.

In Brno 3 June 2021

Malík Viktor, Ing.
reviewer